Paul R. Kiesel, Esq. (SBN 119854)
kiesel@kbla.com
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

HORWITZ, HORWITZ & PARADIS, Attorneys at Law
Paul O. Paradis, Esq.
Gina M. Tufaro, Esq.
Mark A. Butler, Esq.
570 7th Avenue, 20th Floor
New York, NY 10018
Telephone: 212/986.4500
Facsimile: 212/986-4501

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

STEVEN SINACORI, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **HEWLETT-PACKARD COMPANY, a Delaware Corporation,** **Defendant.**	**CASE NO.: 5:11-cv-05779-LHK** **FIRST AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349** **JURY TRIAL DEMANDED**

Plaintiff Steven Sinacori ("Plaintiff") individually and on behalf of all others similarly situated, by his undersigned counsel, alleges the following upon personal knowledge as to his own acts and upon information and belief as to all other matters. Plaintiff's information and belief are based upon the investigation conducted by counsel.

NATURE OF THE ACTION

1. Plaintiff brings this action individually and as a class action against Hewlett-Packard Company ("Hewlett-Packard" or "HP" or "Defendant") on behalf of all others who purchased a Hewlett-Packard LaserJet printer that lacks a "digital signature" or "code signing" security feature (the "HP Printers") in New York State (the "Class").

2. The HP Printers suffer from a defect in the software that is resident on the HP Printers (which is hereinafter referred to as "firmware"). The defective firmware allows computer hackers to install malicious software into the HP Printers simply by sending a print job to the HP Printer because the firmware lacks a critical security measure known as a "digital signature" (also known as "code signing"). The lack of a "digital signature" or "code signing" feature enables hackers to gain access to, take control of, and steal sensitive information from the HP Printers and any other device that communicates with HP Printers.

3. Despite Defendant's knowledge of the fact that the HP Printers could be the subject of attacks by computer hackers, and Defendant's knowledge of the fact that the firmware embedded in the HP Printers lacks a "digital signature" or "code signing" feature, Defendant failed to disclose to Plaintiff and members of the Class that the firmware embedded in the HP Printers lacked the very critical digital signature feature or "code signing" ability that could prevent these attacks.

4. As a result of Defendant's failure to disclose the material fact that the firmware embedded in the HP Printers lacks a "digital signature" feature, Plaintiff and members of the Class were forced to pay more for their HP Printers than they

would have paid had this material information been disclosed. Accordingly, Plaintiff and members of the Class were damaged when they paid a premium for their HP Printers.

5. As a result of the facts alleged herein, Defendant has violated New York law governing consumer protection.

THE PARTIES

6. Plaintiff Steven Sinacori is a resident and citizen of the State of New York. Plaintiff purchased an HP LaserJet Printer model CP2025 during the relevant time period. Plaintiff was unaware that the HP Printer that he purchased suffered from the defect alleged herein. Had Defendant disclosed the existence of the defect before Plaintiff Sinacori purchased his HP Printer, Plaintiff Sinacori would not have purchased the HP Printer and would not have paid a premium for the HP Printer that Plaintiff purchased.

7. Defendant Hewlett-Packard Company is incorporated under the laws of the State of Delaware. Defendant's corporate headquarters is located in Palo Alto, California. Defendant advertises, distributes, markets and sells the HP Printers to tens of millions of consumers throughout United States, including New York State.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over the claims asserted in this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332. Plaintiff, a citizen of New York, brings claims on behalf of a class of all persons who purchased the HP Printers in the State of New York against Defendant, a citizen of California.

9. This Court has jurisdiction over all causes of action asserted herein pursuant to 28 U.S.C. § 1332(d) because the aggregate claims of Plaintiff and members of the Class exceed the sum or value of $5,000,000, and diversity of citizenship exists between at least one member of the proposed Class and Defendant.

/ / /

10. Although Defendant is in possession of information demonstrating the exact size of the Class, Plaintiff believes that at least thousands of people purchased an HP Printer during the Class Period.

11. This Court has personal jurisdiction over Defendant because Defendant maintains sufficient contacts in this jurisdiction, including the marketing and distribution of the HP Printers.

12. Venue is proper in this District because a substantial part of the events and omissions giving rise to the claim occurred in this District, including the marketing and distribution of Defendant's products in this District.

SUBSTANTIVE ALLEGATIONS

The HP Printers and Remote Firmware Updates

13. Hewlett-Packard is the dominant printer seller worldwide, selling approximately 40 million printers annually.

14. Because HP Printers perform some computing functions, firmware is embedded in the HP Printers to help perform specific tasks. Unlike the software in a general-purpose computer, which performs thousands of functions, the firmware embedded in the HP Printers controls the basic functions of the HP Printer.

15. HP recommends that the firmware on the HP Printers be upgraded whenever a firmware upgrade is available. According to HP, "[f]irmware updates add new features as they become available, without the need to change hardware. You can preserve your current investment and still take advantage of the latest tools and capabilities emerging from evolving technology." In addition, upgrading printer firmware can improve the overall performance of the HP Printers, will help the HP Printers operate faster and more efficiently, will fix any firmware or hardware bugs that HP has identified, and can help any compatibility issues the HP Printers may have with other devices.

/ / /

The Defect in the Firmware Embedded in the HP Printers

16. The firmware embedded in the HP Printers suffers from a defect that renders the HP Printers and any computer that communicates with the HP Printers highly vulnerable to attacks by hackers despite the Class member's efforts to implement Internet security measures.

17. In late November of 2011, Ang Cui and Professor Salvatore Stolfo of Columbia University's Intrusion Detection Systems Lab released a video demonstrating the existence of this defect and the resultant security vulnerability affecting the HP Printers.[1] Professor Stolfo explained:

> This presentation is about a very serious and significant vulnerability that we've discovered in HP printer firmware. Printers, like any other embedded device, have computers inside them and run software. . . . . The firmware that runs in HP printers has a significant vulnerability, and we are going to demonstrate the exploitation of that vulnerability and the implications [when] malware [is] injected into the printer firmware. . . ."

18. The "vulnerability" to which Professor Stolfo referred exists because the firmware embedded in the HP Printers lacks a critical security measure known as "code signing" or a "digital signature."

19. "Code signing" or a "digital signature" is a mechanism that is used to verify that a particular digital document or a message is authentic. A digital signature provides the receiver a guarantee that the message or program was actually generated by the sender and that it was not modified by a third party hacker.

20. Accordingly, with respect to the HP Printers, a "digital signature" would be necessary to verify that any remote firmware upgrades sent to the HP Printers are actually generated by HP itself, as opposed to a computer hacker.

---

[1] Columbia Researchers Show Remote HP Printer Hijack, Tim Conneally, November 29, 2011, http://betanews.com/2011/11/29/columbia-researchers-show-remote-hp-printer-hijack-video/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+bn+%28Betanews+Full+Content+Feed+-+BN%29.

21. Without this critical authentication tool, hackers can write phony firmware updates and make them available for download on the Internet. If the user of an HP Printer downloads the phony firmware update, the HP Printer will not be able to recognize that the phony firmware update it is not an authentic HP firmware update.

22. Alternatively, hackers can write encoded commands into documents that are sent to the HP Printers for printing, and once printed, the HP Printer automatically "updates" its firmware with the hackers' malicious software known as malware: *i.e.*, hostile, intrusive, or annoying software or programming code designed to disrupt, steal sensitive information from, gain unauthorized access to, or to achieve other abusive behavior toward, computers and other network devices.

23. HP's failure to use digital signatures to authenticate firmware upgrades gives hackers a wide-open opportunity to reprogram the HP Printers' firmware with their malicious software without detection.

24. According to Professor Stolfo and his research team, infiltration by a computer hacker takes only about 30 seconds, and, during that time, undetectable malware can be installed.

25. Once the malware is installed in the HP Printer, the HP Printer can communicate outward with the Class member's device(s) and the hacker's computer. The connection between the Class member's computer and the hacker's computer gives the hacker a persistent foothold in a secure network undetected by any security measure, such as a "firewall," instituted by a Class member. The HP Printer thereby becomes a beachhead behind the firewall for the hacker, enabling the hacker to run stealthy reconnaissance and attacks from the HP Printer, gaining access to sensitive information.

26. This security vulnerability caused security expert Mikko Hypponen, head of research at security firm, F-Secure, to ask "how the hell doesn't HP have a signature or certificate indicating that new firmware is real firmware from HP?"

Two Methods of Installing the Malware to the HP Printers

27. On December 29, 2011, PhD student Ang Cui and Professor Salvatore Stolfo gave a presentation entitled "Print Me If You Dare: Firmware Update Attack And The Rise of Printer Malware."

28. In this presentation, Ang Cui described two methods that would allow a hacker to install malicious software in the victim's HP Printer: (1) the "reflexive attack" and (2) the "active attack."

A. Reflexive Attack

29. In a "reflexive attack," a Class member may install malware into his or her HP Printer if a hacker embeds malicious software into a document that the Class member is likely to print, such as a resume, picture, coupon, rebate, or an event or transportation ticket, etc. If the Class member prints the "infected" document, then the malicious software update will automatically be installed into the HP Printer.

30. Alternatively, in a "reflexive attack," a hacker could simply place a phony firmware upgrade available for download on a website or in a pop-up window. If the Class member downloads and installs the phony firmware upgrade, then the HP Printer will be infected.

B. Active Attack

31. An active attack is a second method of installing malicious firmware into the victim's HP Printer.

32. An active attack can be performed only if (i) the HP Printer is connected to the Internet and (ii) the HP Printer is not protected by a security feature known as a firewall. When these two conditions are present, the hacker can wirelessly send a print job containing malicious software directly from the hacker's computer to the HP Printer. The hacker can skip the step of tricking the Class member into sending a virus-laced print job to a target printer, as in a reflexive attack.

/ / /

33. In either a reflexive or active attack, the malicious firmware in the HP Printer will instruct the HP Printer to serve as a gateway for communication between the hacker's computer and other devices that communicate to the HP Printer, such as the Class member's computer.

34. For example, if a Class member's HP Printer communicates with other devices through an Internet connection, such as an Ethernet connection or a wireless connection, then malicious software can instruct that HP Printer to communicate directly with the hacker's computer through the Internet connection. The hacker's computer can, in turn, use the HP Printer to establish a connection with any other device that communicates to that particular HP Printer.

35. However, according to a MSNBC article, "[e]ven home users with printers that are not directly connected to the Internet are at risk, Cui said. As long as the printer is connected to a computer – through a USB cable, for example – it could be used to launch attacks, or as part of a botnet." This is because as long as the HP Printer can receive a print job, it can receive a malicious firmware upgrade. Once the HP Printer is infected, it can instruct the computer to which it is connected to perform the security exploits intended by the hacker.

The Defect In The Firmware Of The HP Printers
Has Been Confirmed By Columbia University Researchers

36. Ang Cui and Professor Salvatore Stolfo have confirmed the existence of the defect in the firmware embedded in the HP Printers.

37. In particular, they have confirmed that: (i) the firmware embedded in the HP Printers allows the HP Printers to be updated remotely; (ii) as a result of updating its firmware remotely without code signing or a digital signature, the HP Printers, and the networks on which they are installed, are exposed and vulnerable to attacks; (iii) hackers can infiltrate networks, exfiltrate valuable and sensitive information, and inflict physical damage to the HP Printers themselves; and (iv) the defect impacts millions of HP Printers.

A. The Defect in the Firmware of the HP Printers Exposes Personal and Confidential Information to Theft

38. In his first demonstration in the November 2011 video, Ang Cui caused a form of data-stealing malware called a "print job interceptor" to be installed on an HP Printer. This particular malware forwards to the hacker's printer every print job sent to the HP Printer by the victim. In this demonstration, the victim printed a tax return to the infected HP Printer. The malware installed in the HP Printer intercepted the tax-return, forwarded it to the hacker's printer, and then printed the tax return. The hacker's computer then scanned the document for critical information, such as Social Security numbers, and when it located this information, published the social security number on a Twitter[2] feed.

39. Ang Cui described how he installed the malicious software into the victim's HP Printer:

> I crafted a special file which includes some legitimate document followed by a specially crafted firmware update for this particular printer which includes our stealthy rootkit, exfiltration capability, and reverse IP proxy. All I have to do to infect a [HP] Printer with this malware is to simply print the document to the vulnerable printer. Once the document is sent to the printer, all you will see is that a file begins to print. Immediately after that the printer enters firmware update mode.

40. Ang Cui's demonstration confirms that the defect in the firmware of the HP Printers exposes users' sensitive and confidential information to theft and jeopardizes the safety of their devices.

/ / /

/ / /

/ / /

[2] Twitter is an online social networking service and microblogging service that enables its users to send and read text-based posts of up to 140 characters, known as "tweets."

The Enormous Impact of the Defect

41. An enormous number of HP Printers are affected by this vulnerability. Professor Stolfo stated, "The research is crystal clear. The impact [of the defect] is very large. These devices are completely open and available to be exploited. . . . It's like selling a car without selling the keys to lock it." "It's totally insecure," he said.

42. HP has sold an average of 40 million HP Printers per year since 2005. According to Ang Cui, **the firmware embedded in potentially all of the HP Printers that HP shipped between 2005 to the present is defective. He said, "We are talking about all of the printers that HP shipped that are vulnerable to [the reflexive attack] between . . . 2005 and [the present]. . . . This is not a million. This is not ten million: We are really in the order of potentially hundreds of millions of vulnerable printers**." (Emphasis added).

43. With access to one computer on a network, the hacker could spread malware from the infected computer to any other computer in the network. As noted by security expert Mikko Hypponen, "Many people don't realize that a printer is just another computer on a network with exactly the same problems and, if compromised, the same impact." The defect in the firmware embedded in the HP Printers exposes all other devices to a risk of intrusion, infection, corruption, and exfiltration.

44. Furthermore, infecting an HP Printer is relatively easy, Cui commented, and now that he has proven the existence of the defect, he opined others could reproduce his work in a day or two. "In fact, it's almost impossible to think that someone else hasn't already done this," Cui said.

/ / /

/ / /

/ / /

/ / /

/ / /

HP Has Long Had Knowledge That The HP Printers Are Vulnerable To Attacks By Hackers But Failed To: (i) Takes The Steps Necessary To Protect Against Such Attacks By Programming The Firmware Embedded In The HP Printers To Use Digital Signatures and (ii) Disclose The Material Fact That The Firmware Embedded In The HP Printers Does Not Use Digital Signatures

45. As a result of designing the firmware embedded in the HP Printers, HP has had knowledge that the HP failed to include a "digital signature" or "code signing" feature in the HP Printers.

46. In addition, since at least as early as May of 2006, HP has had knowledge that the HP printers are vulnerable to attacks by hackers. Despite this knowledge, HP failed to: (i) takes the steps necessary to protect against attacks by hackers by programming the firmware embedded in the HP Printers to use digital signatures and (ii) disclose the material fact that the firmware embedded in the HP Printers does not use digital signatures.

47. Although HP knew that the HP Printers were vulnerable to attacks by hackers, HP did not program the firmware embedded in the HP Printers to use digital signatures. Furthermore, despite HP's knowledge of the fact that the HP Printers are vulnerable to attacks by hackers, HP failed to disclose the material fact that the firmware embedded in the HP printers does not use digital signatures.

Hewlett-Packard Is Forced To Publicly Acknowledge The Existence Of The Defect In Firmware Embedded In The HP Printers

48. On or about November 28, 2011, MSNBC published an article exposing the existence of the HP Printer firmware defect and discussing, in detail, the results of the study conducted by Professor Stolfo, Ang Cui and the researchers at Columbia University.

49. In particular, MSNBC reported that HP Printers suffer from a widespread security vulnerability caused by the defect in the firmware embedded in the HP Printers: *i.e.*, the lack of a digital signature.

/ / /

50. This MSNBC article further reported that HP, itself, acknowledged that it has "identified a potential security vulnerability with some HP LaserJet printers."

51. Forced to publically admit the fact that the firmware embedded in the HP Printers is defective because it lacks a digital signature feature, HP finally issued two press releases (the "Press Releases") and a series of security bulletins (the "Security Bulletins") discussing the defect.

A. The Press Releases

52. In a press release issued on November 30, 2011, Hewlett-Packard admitted that (i) a "security vulnerability" in the HP Printers exists; (ii) this "security vulnerability" exposes the HP Printers to "malicious effort[s]" by computer hackers; and (iii) as a result of this "security vulnerability," "it may be possible for a specially formatted corrupt print job to trigger a software upgrade" from an unknown source.

53. HP attempted to downplay the cause of the defect by incorrectly blaming users for not placing their HP Printer behind a firewall. "The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall," HP said. By scanning the Internet for six months with a scanning device, Ang Cui discovered that 76,995 HP Printers were placed on the public Internet without a firewall. Moreover, placing the HP Printer behind a firewall only protects against infection through the "active attack." It offers no protection against the "reflexive attack."

54. On December 23, 2011, HP published the second Press Release stating that, in order to address the defect, "HP has built a firmware update to **mitigate** this issue and is communicating this proactively to customers . . . ." (Emphasis added). Furthermore, HP reiterated "its recommendation to follow best practices for securing devices . . . where possible, disabling remote firmware upload on exposed printers."

55. Despite HP's firmware update, the defect is not eliminated, because the firmware embedded in the HP Printers still lacks a digital signature tool, and the HP Printers remain vulnerable to attacks by hackers.

B. The Security Bulletins

56. HP released Security Bulletin "HPSBPI02728 SSRT100692 rev.1 - Certain HP Printers and HP Digital Senders, Remote Firmware Update Enabled by Default" on November 30, 2011, and released revised versions two and three on December 23, 2011, and January 9, 2012 respectively.

57. Stressing the urgency of the situation, HP placed the following warning at the top of the bulletin:

> "NOTICE: The information in this Security Bulletin should be acted upon as soon as possible."

58. In each version of the Security Bulletin, HP described the defect as follows:

> Remote Firmware Update (RFU): The Remote Firmware Update (RFU) feature is enabled by default. A firmware update can be sent remotely to port 9100 without authentication. This could allow unauthorized modification of the device firmware. The unauthorized firmware could impact the confidentiality and integrity of data sent to and received from the device. The unauthorized firmware could also cause a Denial of Service (DoS) to the device.

59. In revision one of the Security Bulletin, HP informed "Network Administrators" that "[i]t is recommended that the device be secured as described in the document below, including disabling the Printer Firmware Update . . . ."

60. In revisions two and three of the Security Bulletin, HP informed "Network Administrators" that the "RESOLUTION" to the vulnerability was as follows:

> The following steps can be taken to avoid unauthorized firmware updates:
> Update the firmware to a version that implements code signing
> Disable the Remote Firmware Update

> The code signing feature verifies that firmware updates are properly signed. This will prevent the installation of invalid firmware updates.

61. However, in revision three of the Security Bulletins, HP admitted that "A firmware update may be required to allow the RFU to be disabled or to implement code signing," which means that from 2005 until the release of the Security Bulletin, the remote software upgrade feature could not be disabled on some HP Printers and some HP Printers were not capable of recognizing signed code.

HP's Purported "Resolution" is Ineffective

62. The "resolution" described in the Security Bulletins is not, in actuality, a "resolution" for several reasons.

63. First, according to HP, only a "network administrator" should disable the remote embedded firmware upgrade feature. This means that Class members, the majority of which are not "network administrators," will not be able to take advantage of the purported fix.

64. Second, and even worse, this "resolution" still exposes consumers to repeated security vulnerability. Because every time a Class member enables the remote firmware update feature on an HP Printer, the Class member's HP Printer is exposed to the security vulnerability affecting the HP Printers.

65. Third, HP's purported resolution does not remedy those HP Printers which have already been infected by malware that has gained entry to the HP Printer because of HP's lack of the use of a digital signature. Printers that are already compromised by malware cannot be fixed. According to Professor Stolfo, "If and when HP rolls out a fix, if a printer is already compromised, the fix would be completely ineffective. . . ."

/ / /

/ / /

/ / /

Defendant's Failure to Disclose the Existence Of The Defect In the HP Printer Firmware Caused Plaintiff and Class Members To Pay A Premium For The HP Printers

66. Despite Defendant's knowledge of the fact that the HP Printers could be the subject of attacks by computer hackers, and Defendant's knowledge of the fact that the firmware embedded in the HP Printers lacks a "digital signature" or "code signing" feature, Defendant failed to disclose to Plaintiff and members of the Class that the firmware embedded in the HP Printers lacked the very critical code signing ability or a digital signature that could prevent these attacks.

67. As a result of Defendant's failure to disclose the very material fact that the firmware embedded in the HP Printers lacked a "digital signature" feature, Plaintiff and members of the Class were forced to pay more for their HP Printers than they would have paid had this material information been disclosed. Accordingly, Plaintiff and members of the Class were damaged when they paid a premium for their HP Printers.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this action both individually and as a class action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3) against Defendant, on his own behalf and on the behalf of any person who purchased an HP Printer that lacks a "digital signature" or "code signing" security feature in the New York State.

69. Members of the Class are so numerous that joinder of all members would be impracticable. Plaintiff estimates that there are millions of members of the Class.

70. Questions of law and fact are common to all the members of the Class that predominate over any questions affecting only individual members, including:

a. Whether the firmware in the HP Printers is defective;

b. Whether Defendant had knowledge of, but failed to disclose the existence of the defect in the firmware of the HP Printers;

c. Whether Defendant's act of failing to program the firmware embedded in the HP Printers with a "digital signature" feature and Defendant's failure to disclose the existence of this defect in the firmware of the HP Printers was misleading; and

d. Whether as a result of Defendant's misconduct, Plaintiff and other Class members are entitled to damages, restitution, equitable relief, injunctive relief, or other relief, and the amount and nature of such relief.

71. The claims of Plaintiff are typical of the claims of the members of the Class. Plaintiff has no interests antagonistic to those of the Class, and Hewlett-Packard has no defenses unique to the Plaintiff.

72. Plaintiff will protect the interests of the Class fairly and adequately, and Plaintiff has retained attorneys experienced in complex class action litigation.

73. A class action is superior to all other available methods for this controversy because:

i. the prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests;

ii. the prosecution of separate actions by the members of the Class would create a risk of inconsistent or varying adjudications with respect to the individual members of the Class, which would establish incompatible standards of conduct for Defendant;

iii. Defendant acted or refused to act on grounds generally applicable to the Class; and

iv. questions of law and fact common to members of the Class predominate over any questions affecting only individual members, and a class action is

superior to other available methods for the fair and efficient adjudication of the controversy.

74. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT I

(By Plaintiff, Individually and on Behalf of All Class Members, for Violation of the New York General Business Law § 349)

75. Plaintiff incorporates and re-alleges all of the foregoing paragraphs.

76. At all times relevant herein, the New York General Business Law ("GBL") was in effect. GBL § 349 prohibits materially misleading, consumer-oriented business acts that cause injury to the Plaintiff. The deceptive practice must be likely to mislead a reasonable consumer acting reasonably under the circumstances.

77. At all times relevant herein, the HP Printers suffered from a defect in the firmware that is resident on the HP Printers. In particular, the firmware embedded in the HP Printers lacks a critical security measure known as a "digital signature" or "code signing". The lack of a "digital signature" or "code signing" enables hackers to gain access to, take control of, and steal sensitive information from the HP Printers and any other device that communicates with HP Printers.

78. Despite Defendant's knowledge of the fact that the HP Printers could be the subject of attacks by computer hackers, Defendant failed to: (i) take the steps necessary to protect against such attacks by programming the HP Printers to use digital signatures; and (ii) disclose to Plaintiff and members of the Class that the firmware embedded in the HP Printers lacked the very critical code signing ability or a digital signature feature that could prevent these attacks. Defendant's acts and omissions of material fact were misleading.

/ / /

79. As a result of Defendant's acts and failure to disclose the very material fact that the firmware embedded in the HP Printers lacked a "digital signature" feature, Plaintiff and members of the Class were forced to pay more for their HP Printers than they would have paid had this material information been disclosed.

80. Accordingly, Plaintiff and members of the Class were damaged when they paid a premium for their HP Printers.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that this Court:

a. Certify this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, appoint the named Plaintiff as the Class representative, and appoint the undersigned as class counsel;

b. Order Defendant to pay Plaintiff and other members of the Class an amount of actual and statutory damages, restitution and punitive damages in an amount to be determined at trial;

c. Issue a permanent injunction or other appropriate equitable relief requiring ;

d. Issue an order granting Plaintiff's reasonable costs and attorney's fees; and

e. Grant such other relief as may be just and proper.

DATED: February 3, 2012 **KIESEL BOUCHER & LARSON LLP**

By: */s/ Paul R. Kiesel*

Paul R. Kiesel, Esq.
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: 310/854.4444
Facsimile: 310/854.0812

Paul O. Paradis, Esq.

Gina M. Tufaro, Esq.
Mark A. Butler, Esq.
HORWITZ, HORWITZ & PARADIS, Attorneys at Law
570 7th Avenue, 20th Floor
New York, NY 10018
Telephone: 212/986.4500
Facsimile: 212/986-4501

Attorneys for Plaintiff

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

DATED: February 3, 2012

KIESEL BOUCHER & LARSON LLP

By: */s/ Paul R. Kiesel*

Paul R. Kiesel, Esq.
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: 310/854.4444
Facsimile: 310/854.0812

Paul O. Paradis, Esq.
Gina M. Tufaro, Esq.
Mark A. Butler, Esq.
HORWITZ, HORWITZ & PARADIS, Attorneys at Law
570 7th Avenue, 20th Floor
New York, NY 10018
Telephone: 212/986.4500
Facsimile: 212/986-4501

Attorneys for Plaintiff